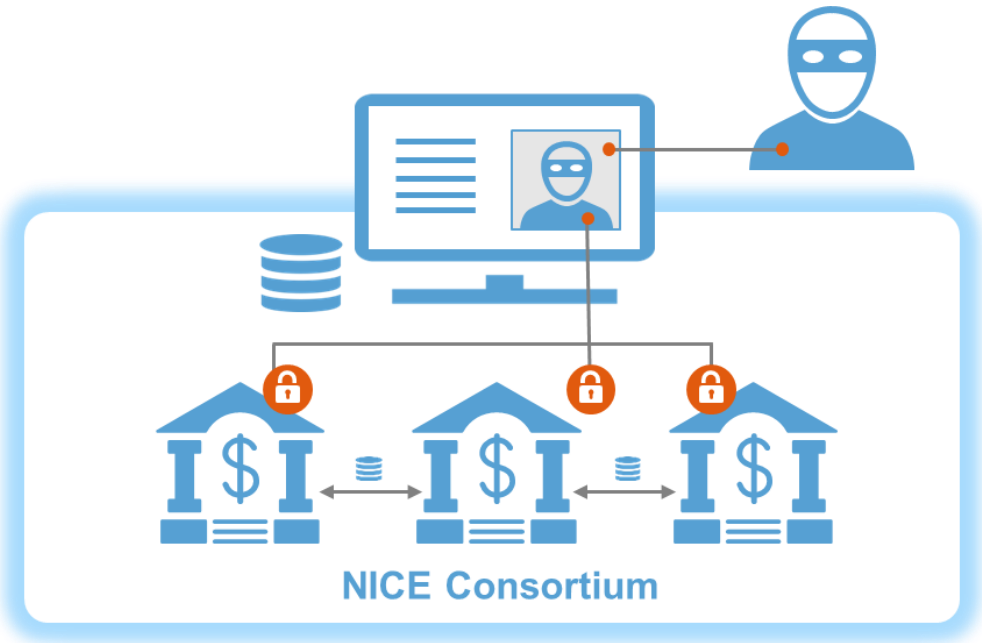
NICE CONTACT CENTER FRAUD PREVENTION FRAUD CONSORTIUM

UNITED STATES PRIVACY OVERVIEW

EXECUTIVE SUMMARY

- NICE Systems is launching a contact center fraud consortium database for financial institutions
- In summary:
  - The database will aggregate voiceprints of identified fraudsters from different financial institutions, to increase each consortium participant's access to known fraudster voiceprints
  - Each participant will be able to share and leverage shared voiceprints via the database, which will be managed by NICE, to increase their fraud prevention capabilities
  - The database will not contain any personal information that can be tied back to the fraudster
- After reviewing and applying existing law to the solution, NICE sees no major impediments to enabling the contact center fraud consortium
- A full overview of the solution, the law and relevant conclusions are contained in this document



Wednesday, August 1, 2013

PROPRIETARY AND CONFIDENTIAL

CONTACT CENTER FRAUD CONSORTIUM
U.S. PRIVACY OVERVIEW

DISCLAIMER: THE INFORMATION CONTAINED IN THIS OVERVIEW IS LIMITED TO U.S. LAW AND IS BELIEVED TO BE CURRENT AS OF THE DATE ABOVE. PRIVACY LAW IS SUBJECT TO RAPID CHANGE, AND NICE BEARS NO RESPONSIBILITY FOR UPDATING THE CONTENT OF THIS OVERVIEW.

THIS OVERVIEW IS NOT INTENDED AS, AND DOES NOT PROVIDE, ANY LEGAL OPINION OR ADVICE. IN THIS REGARD, EACH CUSTOMER IS ENCOURAGED TO OBTAIN ITS OWN LEGAL COUNSEL REGARDING THE APPLICATION OF U.S. PRIVACY AND INFORMATION SECURITY LAWS TO THE SOLUTION.

NICE Systems ("NICE") has proposed development of a voiceprint database analysis tool (the "Solution") that will allow NICE's customers ("Customers") to share potential fraudster information with each other based on a comparison of aggregated voiceprints contributed by Customers from their own customer service call centers to a central database managed by NICE. The Solution is currently in development, and the analysis in this Overview is subject to change relative to changes in the development of the Solution and applicable laws.

1 The Solution

As currently contemplated, the "contact center fraud consortium" would be a loosely organized group of Customers (current focus is on financial institutions only) that subscribe to the Solution, and contribute voiceprint information to the database (the "Consortium"). The concept rests on the premise that Customers currently record incoming customer service calls, create voiceprints of known fraudsters from those calls and, in some instances, run comparisons of the voiceprints against incoming calls to determine if a particular caller seeking authorization to access an account has previously been tagged as a fraudster. The Solution will serve as a repository for a wide range of voiceprints, therefore increasing each participant's access to known fraudster voiceprints. While there are other solutions in the marketplace that are either on-premise installations of analytic software or SaaS products limited to a single customer's inbound calls, NICE wishes to expand and take advantage of a marketplace opportunity for on-demand authentication across customers as fraudsters jump from one call at one institution to another call at another institution. It is further contemplated that NICE will manage the Consortium database either on its premises or at a third party data center, and Customers will access the database through the Solution. Further, Customers will upload their voiceprints to the Solution, and if the voiceprint is not already present in the Consortium, it will be tagged with a unique NICE Fraudster ID and added to the Consortium. Customers will be notified by email alert that a new NICE Fraudster ID has been identified, and can then use the Solution to download the new voiceprint from the Consortium onto their system. If a Customer uploads a voiceprint to the Solution that already exists in the Consortium, NICE will provide the NICE Fraudster ID to that Customer. The voiceprints will be tagged with associated metadata provided by the Customer, including items such as the number of fraud attempts, the audio of the last actual fraud attempt, and the overall rating/score of the voiceprint; however, it is not contemplated that voiceprints would be tagged with any information or metadata which would enable NICE (or anyone else) to associate a name or identity with the voiceprint.

2 The Law

Privacy laws in the United States (as elsewhere in the world) are rapidly changing, and biometric data is an emerging area of regulation. Factors affecting the sharing of information such as voiceprints include:

- The state of residence of the individual voiceprint subject;
- Whether the voiceprint is combined with other personally identifiable information, such as name; and
- The industry-specific regulatory framework (e.g., health, financial services) applicable to the information.

The primary U.S. federal law regulating personal information of customers of financial institutions and their affiliates is known as Gramm-Leach-Bliley, and forms the major platform of this Overview. State laws affecting collection, use and storage of biometric data have also been reviewed and are discussed herein.

A. Gramm-Leach-Bliley Act

In general, the Gramm-Leach-Bliley Act (the "GLBA")[1/] prohibits a "financial institution" from disclosing "nonpublic personal information" about a customer to a nonaffiliated third party, unless the customer has been provided with notice and has had the opportunity to opt out of the disclosure, and the customer has not chosen to opt out or has not otherwise opted-out.[2/] A "customer" is defined as any person to whom the financial institution provides a product or service.[3/] Financial institutions are required to provide opt-outs to customers before they can share nonpublic personal information about those customers, unless the activity falls under one of the specific and narrowly-drawn exceptions included in the statute. Financial institutions generally provide the opportunity to opt-out of such sharing to their customers in the annual privacy notice.

Biometric information is not specifically included in the definition of nonpublic personal information and, as proposed, the voiceprints will be provided without any identifiers, making it unlikely that NICE or anyone else would be able to identify the caller. This arguably places the voiceprints outside of the definition of "nonpublic personal information." As the Solution is currently proposed, a Customer will be providing NICE voiceprints from known fraudsters, who have made two or more fraud attempts on the institution. Due to the amount of potential or actual fraud perpetrated by the caller, the institution uses the recordings of the fraudulent individual to make a voiceprint of the fraudster. As currently proposed, the voiceprint files will contain the actual number of fraud attempts made by the caller, the last fraud attempt and the false/positive rating assigned to the voiceprint. Such callers are not customers trying to access a financial product or service, but instead are fraudsters hoping to exploit weaknesses of the financial institution's authentication mechanism to gain access to accounts that do not belong to them. As such, it is arguable that these callers do not fit into the definition of "customer" and would not receive the protections offered by GLBA.

Looking beyond the definition of "customer" and whether a fraudster could ever be a "customer" for purposes of GLBA analysis, NICE analyzed the Solution with respect to various GLBA exceptions to determine whether information sharing (both with NICE and other Consortium members) would be permissible. The GLBA exceptions are narrow, but could be used to further justify the sharing of the voiceprint information with Consortium members. Importantly, the GLBA includes numerous exceptions that permit a financial institution to disclose nonpublic personal information to a nonaffiliated third party without providing the customer an opportunity to opt out.[4/] The GLBA Privacy Rule provides that financial institutions may provide nonpublic

---

1/ Pub.L. 106–102.
2/ *See* e.g. 17 C.F.R. §248(a)(2) (GLBA Privacy Rule issued by the Securities and Exchange Commission).
3/ Pub. L. 106-102, 15 USC §6827.
4/ *See* 17 C.F.R. §248.13-15.

personal information to a nonaffiliated third party without providing the consumer with notice and an opportunity to opt out in order "to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability."[5/] It is important to note that each of the corresponding regulations[6/] also provides for this fraud exception.

The Solution is a fraud prevention product and, in NICE's analysis, falls within the fraud exception. This exception allows financial institutions under GLBA to provide nonpublic personal information to third parties such as NICE, to protect against or prevent fraud. This sharing would not be subject to the GLBA requirements to either obtain customer/consumer notice or consent or provide an opportunity to opt-out of such sharing and any "general opt-outs" that an institution has received from its customers would not be effective for fraud prevention purposes. In addition, GLBA allows a nonaffiliated third party that receives nonpublic personal information from a financial institution to disclose that information to another nonaffiliated third party if "such disclosure would be lawful if made directly to such person by the financial institution.[7/] The effect of this is that NICE is able to share a voiceprint it receives from a financial institution Customer with other Consortium members and use the information solely for fraud prevention purposes, provided the financial institution Customer itself could lawfully disclose the voiceprint to each Consortium member.

B. Federal Wiretap Act & State Wiretap Laws

The Wiretap Act[8/] limits the ability to record, use, and dispose of recordings of telephone calls. The Wiretap Act allows businesses to record calls if one party to the call consents to the recording. The one-party consent requirement of the Wiretap Act is augmented by some state laws that require the consent of all parties. Currently, a majority of state wiretap laws mirror the federal law and require one-party consent to the recording of the call, but eleven states require the consent of all parties to the call.[9/] Nevada requires prior consent of one party or the consent of all parties; and Vermont does not have a statute on point, but case law indicates a willingness to follow federal law, which requires one-party consent.[10/] Although not specifically addressed in wiretap laws, from a best practices perspective, NICE suggests that Customers consider language for prerecorded messages, such as "This call may be monitored, recorded, and processed for quality assurance and fraud prevention purposes."

C. Laws Regulating Collection of Biometric Identifiers

Illinois and Texas[11/] are the only states at present that have enacted statutes specifically addressing the collection of biometric identifiers, including voiceprints. Each statute requires the express consent of the individual to the collection and use of such biometric identifiers, but they differ in important ways.

(1) Illinois

5/ Public Law 106-102, 15 U.S.C. § 6801 (Section 502(e)((3)(B)

6/ Federal Reserve Board: 12 C.F.R. § 216; Office of Thrift Supervision: 12 C.F.R. § 573, OCC: 12 C.F.R. § 40; Federal Deposit Insurance Corporation: 12 C.F.R. § 332; National Credit Union Administration: 12 C.F.R. § 716; Securities and Exchange Commission: 17 C.F.R. § 248; Commodity Future Trading Commission: 17 C.F.R. § 160.

7/ Public Law 106-102, 15 U.S.C. §6801 (Section 502(c)).

8/ 18 U.S.C. §§ 2510-2521.

9/ California, Delaware, Hawai'i, Louisiana, Maryland, Massachusetts, Michigan, Montana, New Hampshire, Pennsylvania and Washington.

10/ *State v. Fuller*, 503 A. 2d 550, 551 (Vt. 1985).

11/ 740 ILCS 14/1-99 and Tex. Bus. & Com. Code §503.00.

The Illinois "Biometric Information Privacy Act" applies to private entities that collect or obtain biometric information or biometric identifiers, such as voiceprints. The Illinois law imposes various obligations relating to consent before collecting, capturing, purchasing or otherwise obtaining a person's biometric identifier or biometric information. The Illinois statute provides an exception for government agencies and financial institutions that are subject to GBLA.

(2) Texas

The Texas statute states that a person who possesses a biometric identifier for a commercial purpose may not "sell, lease or otherwise disclose the biometric identifier" unless the individual consents to the disclosure. The entity is also required to use reasonable care in the protection of the biometric identifier, and to destroy the identifier within a "reasonable time," but no later than one year after the purpose for collection expires. Unlike the Illinois statute, the Texas law does not provide exceptions.

Obtaining consent from a fraudster presents challenges; however, the prerecorded statement discussed above could arguably be used to satisfy the requirements of the Texas law because the caller gives his or her consent to the recording and processing of the call for fraud prevention purposes. The prerecorded statement puts callers on notice that the call is not only being recorded, but also being processed for fraud prevention purposes. Creating voiceprints from the call falls under "processing" and sharing the voiceprints within the Consortium is for the purpose of fraud prevention.

3 Conclusion

Applying existing law to the assumptions relating to the Solution as currently contemplated, NICE sees no major impediments to NICE's receipt of, storage, or use of voiceprints to enable the "contact center fraud consortium." Some regulatory compliance issues will be the responsibility of Consortium members, such as issues of "assumed" consent for the recording and storage of calls and related information from individuals calling into the call centers of Consortium members. NICE envisions a Consortium membership or subscription agreement that addresses these issues. NICE will implement and maintain a comprehensive, written information security program that includes industry-standard administrative, technical and physical safeguards to protect the Consortium information and the voiceprints.

4 Appendix

1/ *Pub.L. 106–102.*
2/ *See e.g. 17 C.F.R. §248(a)(2) (GLBA Privacy Rule issued by the Securities and Exchange Commission).*
3/ *Pub. L. 106-102, 15 USC §6827.*
4/ *See 17 C.F.R. §248.13-15.*
5/ *Public Law 106-102, 15 U.S.C. § 6801 (Section 502(e)((3)(B)*
6/ *Federal Reserve Board: 12 C.F.R. § 216; Office of Thrift Supervision: 12 C.F.R. § 573, OCC: 12 C.F.R. § 40; Federal Deposit Insurance Corporation: 12 C.F.R. § 332; National Credit Union Administration: 12 C.F.R. § 716; Securities and Exchange Commission: 17 C.F.R. § 248; Commodity Future Trading Commission: 17 C.F.R. § 160.*
7/ *Public Law 106-102, 15 U.S.C. §6801 (Section 502(c)).*
8/ *18 U.S.C. §§ 2510-2521.*
9/ *California, Delaware, Hawai'i, Louisiana, Maryland, Massachusetts, Michigan, Montana, New Hampshire, Pennsylvania and Washington.*
10/ *State v. Fuller, 503 A. 2d 550, 551 (Vt. 1985).*
11/ *740 ILCS 14/1-99 and Tex. Bus. & Com. Code §503.00.*